

REMARKS/ARGUMENTS

Claims 1-64 are pending in this application, all of which stand rejected as a result of the January 21, 2004 Office Action. Following entry of the amendment, claims 1, 33, and 54 will have been amended, and claim 5 will have been cancelled. Claims 13 and 64 have been rejected under 35 U.S.C. § 112, second paragraph as being indefinite. Claims 1-9, 11-27, 30-50, 52-54, 56-61, and 63-64 have been rejected under 35 U.S.C. § 102(b) as being anticipated by U.S. Patent No. 5,708,780 (Levergood). Claims 28, 29, and 55 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Levergood in view of U.S. Patent No. 5,970,475 (Barnes). Claims 10, 51, and 62 have been rejected under 35 U.S.C. § 103(a) as being unpatentable over Levergood in view of U.S. Published Patent Application 2001/0011238 (Eberhard).

The cover sheet accompanying the January 21, 2004 Office Action indicates that claims 12, 13, and 64 have been objected to. However, no objection to any claims appears in the text of the Office Action, and thus applicants will assume that the cover sheet is in error.

In view of the amendments and remarks contained herein, applicants submit that all of the claims are patentable, and thus request reconsideration of the Office Action.

Section 112 Rejections of Claims 13 and 64

Applicants respectfully submit that claims 13 and 64 are definite, and request reconsideration of the rejection of these claims under section 112, second paragraph.

With regard to claim 13, the Examiner states that the claim is indefinite because "claim 12 recites the second computing device is transmitting the encrypted information to the first computing device." The Examiner's characterization does not correctly describe the language of claim 12; more importantly, however, it is unclear how this characterization bears on the definiteness of claim 13. Claim 12 recites a method that makes use of (1) encrypted information, (2) a first computing device, and (3) a second computing device. Claim 13 recites that the first computing device is associated with a purchaser of content, and that the second computing device provides the content. There is nothing indefinite about this language.

With regard to claim 64, the Examiner appears to find some inconsistency in the notion that a second server could receive parameters that contain the address of a first server. There is nothing indefinite in this feature. A server is capable of receiving any sort of information – including the address of another server.

Applicants thus submit that claims 13 and 64 are not indefinite, and respectfully request that the rejection of these claims under section 112, second paragraph, be withdrawn.

The Section 102 and 103 Rejections

The independent claims, and several dependent claims, have all been rejected as being anticipated by Levergood. Certain dependent claims have been rejected as being obvious over a combination of Levergood with either Barnes or Eberhard. Applicants respectfully submit that the independent claims (as amended, in certain cases) are not anticipated by Levergood, and thus applicants focus the Examiner's attention on the differences between Levergood and the independent claims.

Levergood describes a system in which certain documents that can be requested by a web-browser are subject to controlled access. The mechanism that is used to control access is a construct referred to in Levergood as a "session identification" or "SID." For example, during a browsing session a user may request the document located at Uniform Resource Locator (URL) <http://content.com/report>. (See col. 5, ll. 42-65.) Access to this document may be restricted, and in order to access the document the user may instead need to issue a request for the URL [http://content.com/\[SID\]/report](http://content.com/[SID]/report).

If the user requests a document that requires an SID and no SID is present in the URL, then the user's request is redirected to an authentication server to generate an SID. (Col. 5, ll. 46-49.) The authentication server then engages in an authentication procedure with the user. (See col. 6, l. 27 through col. 7, l. 21.) If the authentication procedure indicates that the user is entitled to an SID, then the SID is generated, and the authentication server issues a "redirect" instruction to redirect the user to the requested URL with the SID added (e.g., if the user requested

<http://content.com/report>, then the authentication server redirects the user to [http://content.com/\[SID\]/report](http://content.com/[SID]/report).) (Col. 7, ll. 15-21.)

The SID preferably comprises a character string that encodes an expiration date, a key identifier, a domain describing information files to which the SID authorizes access, a user identifier, and a signature which contains a cryptographic hash and an IP address encrypted with a secret key. The only encrypted component of the SID is the encrypted IP address.

Independent Claim 1

Claim 1, as amended Claim 1 calls for “creating an HTTP request which includes an address ... and ... encrypted information,” and “transmitting a web page comprising said HTTP request to a second computing device. Neither Levergood, nor the Barnes and Eberhard references cited, teaches or suggests this feature. As described above, Levergood arguably encrypts information that is included in the SID that later forms part of an HTTP request (e.g., [http://content.com/\[SID\]/report](http://content.com/[SID]/report)). However, Levergood does not transmit the HTTP request to another device as part of a web page. In Levergood, when a user issues an HTTP request without the SID, an authentication server may create a new URL with the SID inserted and may then redirect the user’s browser to the new URL. However, Levergood does not create a new request for inclusion in the web page, and then transmit the web page to a computing device. This difference between Levergood and claim 1 affects the flow of information: in claim 1, the user is given a web page containing a request link that the user may either follow or not follow; in Levergood, the user is not given a choice to follow the link but is simply redirected to another page at the behest of the authentication server.

Thus, none of the prior art cited teaches or suggests the features of claim 1, as amended, and applicants respectfully request that the rejection of claim 1 be reconsidered and withdrawn.

Independent Claim 12

Claim 12 calls for “encrypting information such that the encrypted information is decryptable by a secret,” and further calls for the encrypted information to be transmitted to a

“second device,” and for the secret to be shared with a “first device” for which the information is ultimately destined, but for the secret not to be shared with the second device. In particular, claim 12 calls for the feature “wherein said secret is not accessible to either said second computing device or said user [who operates said second computing device].” This feature as to how the secret is shared (and not shared) is not taught or suggested by Levergood, or any of the other prior art cited.

In Levergood, as discussed above, the only encrypted information is a portion of the SID. Levergood specifies that the “secret key” used to encrypt this information is “shared by the authentication and content servers.” (Col. 5, ll. 64-65.) These two servers are the devices that have access to the SID: the SID is created on the authentication server, and is then transmitted to the content server as a result of the authentication server’s redirect instruction. Claim 12, by contrast, calls for the encrypted information to be transmitted to a “second device” that does not have access to the secret. Since Levergood never shares the encrypted information with a device that does not share the secret, this feature runs contrary to Levergood.

Additionally, Levergood is silent as to whether the secret is actually withheld from any particular device. Claim 12 specifically requires that the secret is not accessible either to the second device or to the user who operates that device. Levergood states that the secret is shared by the authentication and content servers, but does not discuss whether access is withheld from any other device. In other words, Levergood’s silence on this issue means that there may, or may not, be a device to which access to the secret is withheld. This silence is in contrast to claim 12, which requires that the encrypted information be transmitted to a device that does not have access to the secret. Levergood’s silence on this issue does not constitute a teaching to the effect that the secret is withheld from a device. Thus, Levergood cannot be found to anticipate the feature of claim 12 that requires the secret to be inaccessible to a particular device.

Thus, Levergood does not teach or suggest the features of claim 12, and applicants respectfully request that the rejection of claim 12 be reconsidered and withdrawn.

Independent Claim 24

Claim 24 calls for providing two sets of computer-executable instructions to two different parties, for use on two different computing devices. The first set of instructions “encrypts information based on a unique id that maps into a shared secret.” The second set of instructions decrypts the encrypted information.” In other words, claim 24 is about using a multi-party software distribution scheme to facilitate content distribution. The first party receives software that knows how to encrypt information in a certain way, and the second party receives software that knows how to decrypt the information that was encrypted by the first party’s software. Thus, by means of distributing different software to different parties, the second party is enabled to decrypt information that was encrypted by the first party. Neither Levergood, nor any of the other art cited, teaches or suggests this software distribution framework.

Levergood discusses the use of SIDs, and mentions that a portion of the SID may be encrypted. As discussed above, the SID is created by the authentication server and later transmitted to the content server, where it appears to be decrypted. However, there is no discussion in Levergood as to what kind of software is used on the content and authentication servers, or how (or to what parties) it is distributed. In Levergood, the authentication server and the content server are part of the same organization; Levergood does not teach the distribution of two (complementary) pieces of cryptographic software to two different parties.

Thus, Levergood does not teach or suggest the features of claim 24, and applicants respectfully request that the rejection of claim 24 be reconsidered and withdrawn.

Independent Claim 33

Claim 33 is directed to a method of building a client-server request comprising. “First information” is encrypted, and then the request is built by including the encrypted information and the address of a first server. The request is then transmitted to a client, on which the request may be executed. Neither Levergood, nor any of the other cited art, teaches or suggests this feature.

As discussed above, Levergood’s authentication server creates a URL that includes an SID needed to access a particular document, and then redirects the user’s browser to that URL.

The request itself is never transmitted to the user's browser, and is never executed by the browser; rather, the authentication server merely redirects the user's request to the new URL.

Thus, Levergood does not teach or suggest the features of claim 33, and applicants respectfully request that the rejection of claim 33 be reconsidered and withdrawn.

Independent Claim 44

Claim 44 calls for "encrypted information" that is provided by a "first computing device" to a "second computing device." Moreover, the relationship between the first and second computing devices is as follows: the first computing device receives an order for a content item from the second computing device. This relationship between the first and second computing devices represents a distinction between claim 44 and Levergood.

In Levergood, the user requests a document from the content server (e.g., <http://content.com>). However, if the requested document requires an SID, then the user is redirected to the authentication server, so that the authentication server may provide the SID. As discussed above, the SID is the only structure in Levergood that contains encrypted information. Thus, the encrypted information in Levergood is not provided by the device at which an order for a content item is placed, but rather is generated by a different device. Levergood decouples the functions of receiving orders for content and generating the encrypted information that is needed to provide that content; claim 44, by contrast, merges these two functions into a single machine. Levergood's decoupling of the encryption and content-ordering functions represents a substantial difference between claim 44 and Levergood.

Thus, Levergood does not teach or suggest the features of claim 44, and applicants respectfully request that the rejection of claim 44 be reconsidered and withdrawn.

Independent Claim 54

Claim 54 calls for "encrypting one or more" parameters that "identify characteristics of a first transaction between a first client and a first server." Claim 54 further calls for returning the encrypted parameters to the "first client. Additionally, claim 54, as amended, calls for returning

the transaction to be a purchase transaction. None of these features are taught or suggested by Levergood, or any of the other prior art cited. In particular, these features differ from Levergood for at least two reasons.

First, as discussed above, Levergood's encrypted information (i.e., a portion of the SID) is not transmitted between the parties who engage in a transaction. Even if one assumes that a user's requesting a document is a "transaction" in the sense of claim 54, the user would be the "client" in that transaction, and the SID is not transmitted to the client; rather, as discussed above, the authentication server redirects the user's browser to a URL that contains an SID generated by the authentication server.

Second, inasmuch as claim 54 calls for the transaction to be a purchase transaction, this feature is clearly absent from Levergood. Levergood indicates that the documents requested by users are controlled-access documents (e.g., private reports), but does not indicate that the users are *buying* those documents.

Thus, Levergood does not teach or suggest the features of claim 54, and applicants respectfully request that the rejection of claim 54 be reconsidered and withdrawn.

Dependent Claim 20

As described above in connection with claim 1, Levergood does not create a web page that includes encrypted information as part of an HTTP request. Inasmuch as claim 20 calls for a similar feature, claim 20 is patentable for the same reasons as claim 1.

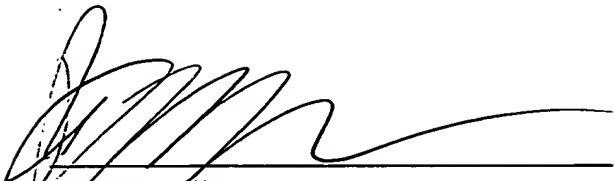
Drawings

The Examiner has not indicated whether the formal drawings filed with this application are acceptable. It is requested that the Examiner indicate in the next Office Action that the formal drawings are acceptable.

DOCKET NO.: MSFT-0127
Application No.: 09/604,944
Office Action Dated: January 21, 2004

PATENT

Date: April 23, 2004


Peter M. Ullman
Registration No. 43,963

Woodcock Washburn LLP
One Liberty Place - 46th Floor
Philadelphia PA 19103
Telephone: (215) 568-3100
Facsimile: (215) 568-3439